

CASE STUDY

Government Contractor

A government contractor that provides security detail for the Department of Defense and high profile homeland security missions uses Atakama to secure confidential data received from the government based on their work. As a result, they are required by ITAR regulatory requirements to ensure this highly sensitive information is safely protected and inaccessible to any non-US citizen.

The Need

In light of the volume of sensitive data they possess and interact with on a daily basis, our client needed to ensure they can employ the highest level of security without incurring workflow frictions or disruptions to expected behavior and interaction with their files. The solution had to be easy and quick to implement in a short period of time. Traditional encryption solutions would not solve their use-case, as they are connected to user credentials/IAM which can be easily compromised by an attacker.

The Approach

Using Atakama, the government contractor will now be able to encrypt each file with its own AES256 bit key. And because Atakama does not rely on existing file access controls, its encryption and security are detached from identity and access management. The result is a standalone solutions that does not bulk decrypt every file the minute a user logs onto their computer, which is something many regulators are requiring at a greater rate.

The Result

The client chose to use Atakama because it is incredibly easy to use, was deployed quickly, and keeps confidential files encrypted at all times, even when users are logged into the contractor's network. The client has leveraged Atakama's multi-factor encryption software to ensure that their confidential data remains secure even when the security perimeter may fail.